State Privacy Laws: Not As Comprehensive As You May Think

By **Liisa Thomas** (September 19, 2023)


Liisa Thomas

As more and more U.S. states enact privacy laws that are often referred to as comprehensive, companies are grappling with how to comply with a rapidly evolving landscape.

Many are hoping that one law can be identified as the most stringent so that compliance efforts can be focused on understanding and adhering to that law's requirements.

Unfortunately, in the U.S., privacy and data security compliance is not that simple.

Privacy and Security Laws and Enforcement: Beyond Comprehensive Laws

The U.S., unlike many other jurisdictions, takes a multiprong approach to privacy legislation.

There are laws at both the state and federal level that apply to companies depending on the industry the company is in, the activity in which it engages, and the individuals whose information is collected and used. In many circumstances, more than one set of laws will apply to an organization.

In the first category are laws like the Health Insurance Portability and Accountability Act, for health care providers, or the Gramm-Leach-Bliley Act, for financial services companies.

In the second are laws like the CAN-SPAM Act, which regulates email marketing; the Biometric Information Privacy Act, which affects the collection of biometric data; or the Song-Beverly Consumer Warranty Act, which affects the collection of personal information during a credit card transaction.

And in the third are laws like the Children's Online Privacy Protection Act, which governs the collection of information from children online.

These are just a few examples. There are hundreds of privacy laws in the U.S. at both the state and federal level, and in some cases, more at a local — city or county — level as well.

In addition to privacy legislation, there are also data security obligations. These might include obligations to protect sensitive data in motion and at rest, as well as an increasing number of laws that require having reasonable written data security policies in place.

In the U.S., many companies find that the laws themselves do not provide sufficient detail about how to protect information such that a written program can be developed. Instead, they look to industry guidelines and standards to develop their programs.

Also of prime concern for U.S. companies on the security side are data breach notification laws. These laws do not impose data security obligations: Instead, they oblige companies to notify if information has been accessed, acquired or used by an unauthorized individual.

In many cases, this occurs because of insufficient protections. Or, at least, that is the theory

for regulators and class action plaintiffs.

As a result, companies' security programs will often focus on how to protect information such that notifications do not become necessary.

On top of the legislative requirements, U.S. companies need to keep in mind that they are in a common law country.

In other words, there is case law that courts follow that creates another — often more stringent — set of requirements. Many of these privacy- and security-related expectations have been created by cases brought under concepts of deception and unfairness.

For deception, claims might be that if a company has been engaged in a deceptive practice because it has said that information will be treated in one way, then it does something different with it.

For unfairness, this includes if the company has engaged in a fundamentally unfair practice by using information in a particular way, or failing to do something with information — usually for the latter, this means allegedly failing to provide enough protections. Unfairness is often alleged after a data breach, on the grounds that the situation occurred because information was not sufficiently protected.

There is one federal agency in the U.S. that has led the way in this space: the Federal Trade Commission. It has brought privacy cases since the early 1990s, prior to the enactment of many federal and state privacy laws.

State attorneys general have also brought their fair share of privacy-related unfairness and deception cases.

Comprehensive State Privacy Laws: Not That Comprehensive

Many of us refer to the new U.S. state privacy laws as comprehensive laws.

We think of them as following the European Union's General Data Protection Regulation, which does address all aspects of the collection, use, storage and protection of personal information.

While many countries around the world have followed the European approach, these U.S. state laws are not as comprehensive. Notably, these laws tend not to address marketing requirements — apart from some digital tracking aspects of marketing.

For example, the laws do not require that companies get consent before sending marketing emails or texts, or give people the right to opt out of such communications.

Those requirements exist, but under other U.S. laws, as noted in the section above. They also do not address data breach notification or data security obligations. Instead, those are addressed under separate U.S. state laws.

Finally, all of the laws have a number of exceptions, like if the company fails to meet financial thresholds or is otherwise regulated under specialty privacy laws like HIPAA or the GLBA.

Having these obligations exist in different laws — as opposed to these comprehensive state

privacy laws — is unlike Europe's GDPR, which does contain those elements.

So then, what is included? The laws obligate companies to provide consumers with certain rights, like the right to access their information and have it corrected. It also gives data deletion rights.

There are, as in Europe, exceptions to when these rights apply. For example, if the information is still needed to carry out a consumer's request, or if there are other legal obligations requiring data retention.

These laws, like the GDPR, impose contracting obligations.

Companies hiring third parties to collect or process information on their behalf will have certain clauses to include in the contracts with those companies. These include instructing vendors on how to use information, that the information is protected and kept confidential, and that vendors cooperate with ongoing assessments and audits of their compliance.

Where are these laws? As most have been tracking, these laws are in effect in California, Colorado, Connecticut and Virginia.

The only other state to go into effect in 2023 will be Utah, on Dec. 31.

In 2024, four more states' laws will go into effect: for Florida, Oregon and Texas, on July 1, 2024, and for and Montana, on Oct. 1, 2024. In 2025, three more: Delaware and Iowa, on Jan. 1, 2025, and Tennessee, on July 1, 2025.

Finally, Indiana's law will be effective on Jan. 1, 2026.

Why Not Take a Most Stringent Law Approach?

With this legislative and enforcement background, we can see that there are hundreds of laws that might apply to an organization.

As noted at the outset, the understandable desire might be to identify which are the most stringent and to focus compliance efforts on those laws. There are a few problems with this approach.

Perhaps most importantly, each of the laws takes a slightly different approach to the content they cover, with some more stringent than others on certain aspects.

Additionally, some states impose certain procedural requirements, like providing rights, that a company might not want to offer globally. Or, the procedural requirements might not be the same from state to state — this is more rare.

Finally, we have to keep in mind that these laws do not cover all of the privacy and data security requirements that exist under U.S. laws.

With this in mind, rather than a most stringent laws approach, companies might want to take a most stringent content approach. In other words, pulling from each of the U.S. state comprehensive privacy laws their most stringent aspects.

As companies do this, what are some of the similarities and differences to keep in mind? Listed below are considerations to keep in mind.

Notice

These laws all have content requirements, with California perhaps having the most detailed.

Required information includes, by way of example, the categories of information being processed by the company, what rights consumers have and what information might be shared.

Beyond privacy policy notice requirements, though, keep in mind that the laws have some on-screen or just-in-time notice requirements when collecting information. This includes information about digital tracking activities as well as financial incentives and information sales.

Choice

Companies under these laws have obligations to let consumers opt out of information sales and online behavioral advertising, sensitive information processing, online behavioral targeting, and profiling that creates a legal or similar impact.

Sales and Targeted Digital Advertising

These U.S. state comprehensive privacy laws are the first in the U.S. to really focus on the concept of selling information. Before these laws, there were data broker laws, but often companies found that they did not fall under the definition of a broker.

The concern when the laws were drafted was particularly focused on exchanging information with third parties not only for money, but also for other consideration, especially in the digital advertising space. There are two major divides in these laws.

First, only half defines a sale as an exchange of other valuable consideration, including California, Colorado, Connecticut, Florida, Montana and Texas.

Second, while all provide for letting people opt out of the sale of their information, only California, Colorado and Connecticut go into details.

Combining these two, a globalized approach to addressing sales and targeting would focus on following the requirements in these three jurisdictions.

Companies evaluating their sales practices should keep in mind that targeted digital advertising is not only a sales issue. Even if the advertising is conducted without any selling, these laws have requirements. These are in addition to existing self-regulations and enforcement under concepts of unfairness and deception.

Sensitive Information

States are divided in their approach to companies' collection of sensitive information.

Some — Colorado, Connecticut and Iowa — require consent to process sensitive information. California on the other hand is more lenient, requiring that companies notify individuals of the processing of sensitive information and give them the ability to opt out.

California has fairly detailed requirements about the notice, and both California and

Colorado have detailed requirements about how to handle an opt-out request.

Profiling

Profiling is generally viewed by these states' laws as automatically evaluating information to predict behaviors or interests.

All but Iowa and Utah give individuals the right to opt out of profiling and impose risk assessment obligations on companies that engage in profiling.

Rights

These laws impose an obligation to provide rights of access/portability, correction — in all but Iowa — and deletion.

Being universal in providing rights to consumers in all states is probably the easiest approach, but there are differences between when exceptions might apply. Some, for example, say that they do not need to be provided if they are technically infeasible or impossible, including California, Connecticut, Iowa, Montana, Tennessee and Utah.

Where the laws differ the most is in the processing of rights.

For example, half allow people to make just one request a year, while the rest — California, Florida, Iowa, Tennessee, Texas and Virginia — allow people to make two each year.

Companies will have to keep these differences in mind when developing their rights approach.

Vendor Contracts

The state privacy laws are mostly uniform in the provisions to include in vendor contracts. These include things like instructions on how to process data, and confidentiality requirements.

There are some differences. Colorado, Connecticut and Iowa require getting written permission before engaging subcontractors, for example.

Record-Keeping

While California has the most detailed set of record-keeping requirements, Colorado has several requirements that go beyond what we see in California.

For example, in Colorado, companies must keep records of opt-out requests, keep records in a readable format and use reasonable security for records kept.

Other requirements are similar across all states, like keeping a record of deletion requests.

Conclusion

It may be easiest to think of these new U.S. state comprehensive laws as adding to, rather than replacing, the existing U.S. privacy law patchwork. And, note that none of these laws is more stringent than others.

Instead, each has stringent aspects to pay attention to.

Keeping this in mind, companies can move forward to not only identify the most stringent aspects of these state laws, but also fit them into the existing privacy and data security law framework.

Liisa Thomas is a partner and leader of the privacy and cybersecurity team at Sheppard Mullin Richter & Hampton LLP.